(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 691 232**

(51) Int. CI.:

G06F 21/62 (2013.01)
G06F 17/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.10.2015 PCT/US2015/057435**

(87) Fecha y número de publicación internacional: **06.05.2016 WO16069508**

(96) Fecha de presentación y número de la solicitud europea: **27.10.2015 E 15794393 (7)**

(97) Fecha y número de publicación de la concesión europea: **25.07.2018 EP 3213248**

(54) Título: **Control de acceso basado en datos de caducidad de operación**

(30) Prioridad:

30.10.2014 US 201414529063

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.11.2018

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052-6399, US

(72) Inventor/es:

PLUMB, GRAHAM CHARLES y
KEYES, WARREN LESLIE

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Control de acceso basado en datos de caducidad de operación

Antecedentes

Los sistemas informáticos y redes asociadas han revolucionado la manera en la que los seres humanos trabajan, juegan y se comunican. Pronto cada aspecto de nuestras vidas se verá afectado de alguna manera por los sistemas informáticos. La proliferación de redes ha permitido que los sistemas informáticos compartan datos y se comuniquen, lo que aumenta enormemente el acceso de la información. Por esta razón, la era actual a menudo se denomina como la "era de la información".

Sin embargo, en algunos casos, es deseable restringir el acceso a los datos. Por ejemplo, los datos a menudo se restringen de modo que únicamente son accesibles por ciertos individuos. Estos individuos por lo tanto deben autenticarse antes de acceder a los datos. En otras circunstancias, los datos se han de restringir basándose en la localización. Por ejemplo, algunos datos se han de confinar en cierto territorio geográfico. La confinación de los datos a una región geográfica particular puede realizarse por una diversidad de razones, tales como razones legales, normativas, de impuestos o de seguridad. En algunos casos, los datos tienen una cierta caducidad asociada con los datos, para restringir cuándo pueden usarse los datos.

La materia objeto reivindicada en el presente documento no está limitada a las realizaciones que resuelven cualesquiera desventajas o que operan únicamente en entornos tales como aquellos anteriormente descritos. En su lugar, estos antecedentes se proporcionan únicamente para ilustrar un área de tecnología ejemplar donde pueden ponerse en práctica algunas realizaciones descritas en el presente documento. El documento de las técnicas anteriores EP-0715243-A desvela un sistema y procedimiento para controlar el acceso a una entidad de sistema de ficheros en dependencia de la información de localización y datos de caducidad asociados con elementos del sistema de ficheros.

Breve resumen

Al menos algunas realizaciones descritas en el presente documento se refieren al control de acceso a una entidad de sistema de ficheros basándose en la localización del solicitante y datos de caducidad de operación de la entidad de sistema de ficheros. Los datos de caducidad de operación y datos de localización están asociados con una entidad de sistema de ficheros (por ejemplo, un fichero, un directorio, una partición, o un disco) de manera que la entidad de sistema de ficheros y los datos de caducidad de operación y los datos de localización se mueven o copian de manera atómica juntos. Tras recibir una solicitud para realizar una operación en la entidad de sistema de ficheros, el sistema identifica un estado de localización del solicitante. El sistema a continuación identifica datos de caducidad que corresponden al estado de localización, y que está asociado con la operación solicitada. El sistema a continuación usa los datos de caducidad identificados para determinar si se ha de permitir o no la operación de fichero solicitada.

Este resumen no se pretende para identificar características clave o características esenciales de la materia objeto reivindicada, ni se pretende que se use como una ayuda al determinar el alcance de la materia objeto reivindicada.

Breve descripción de los dibujos

Para describir la manera en la que pueden obtenerse las anteriormente descritas y otras ventajas y características, se presentará una descripción más particular de diversas realizaciones por referencia a los dibujos adjuntos. Entendiendo que estos dibujos representan únicamente realizaciones de muestra y no se han de considerar por lo tanto que limitan el alcance de la invención, las realizaciones se describirán y explicarán con especificidad adicional y detalle a través del uso de los dibujos adjuntos en los que:

La Figura 1 ilustra de manera abstracta un sistema informático en el que pueden emplearse algunas realizaciones descritas en el presente documento;
La Figura 2 ilustra un sistema en el que un sistema solicitante solicita realizar una operación en una entidad de sistema de ficheros que se encuentra en un sistema de ficheros de un sistema de origen;
La Figura 3 ilustra un entorno de entidad de sistema de ficheros en el que la entidad de sistema de ficheros y los correspondientes datos de localización y datos de caducidad de operación están asociados de tal manera que si la entidad de sistema de ficheros se copia o se mueve, los correspondientes datos de localización y datos de caducidad de operación se copian o se mueven también de manera atómica, respectivamente.
La Figura 4 ilustra datos complementarios que representan un ejemplo de los datos de localización y los datos de caducidad de operación de la Figura 3;
La Figura 5 ilustra de manera abstracta un campo de territorio que representa un ejemplo de cualesquiera de los campos de territorio de la Figura 4;
La Figura 6 ilustra un diagrama de flujo de un procedimiento para controlar el acceso a datos basándose en la localización del solicitante y datos de caducidad de operación; y
La Figura 7 ilustra un procedimiento más específico para controlar el acceso a una entidad de sistema de ficheros basándose en el estado de localización del solicitante y basándose en datos de caducidad específicos

de operación.

Descripción detallada

Al menos algunas realizaciones descritas en el presente documento se refieren al control de acceso a una entidad de sistema de ficheros basándose en la localización del solicitante y datos de caducidad de operación de la entidad de sistema de ficheros. Los datos de caducidad de operación y datos de localización están asociados con una entidad de sistema de ficheros (por ejemplo, un fichero, un directorio, una partición, o un disco) de manera que la entidad de sistema de ficheros y los datos de caducidad de operación y los datos de localización se mueven o copian de manera atómica juntos. Tras recibir una solicitud para realizar una operación en la entidad de sistema de ficheros, el sistema identifica un estado de localización del solicitante. El sistema a continuación identifica datos de caducidad que corresponden al estado de localización, y que está asociado con la operación solicitada. El sistema a continuación usa los datos de caducidad identificados para determinar si se ha de permitir o no la operación de fichero solicitada. En algunas realizaciones, los datos de caducidad identificados para ese estado de localización enumeran caducidades de las mismas operaciones, de manera que una operación puede tener una caducidad diferente que otra, incluso para el mismo estado de localización del solicitante, y para la misma entidad de sistema de ficheros en la que se está operando. Se describirá un análisis introductorio de un sistema informático con respecto a la Figura 1. A continuación, la estructura y uso del control de acceso se describirán con respecto a figuras posteriores.

Los sistemas informáticos cada vez más están tomando una amplia diversidad de formas. Los sistemas informáticos pueden ser, por ejemplo, dispositivos portátiles, aparatos, ordenadores portátiles, ordenadores de sobremesa, ordenadores centrales, sistemas informáticos distribuidos, centros de datos, o incluso dispositivos que no se han considerado de manera convencional un sistema informático, tales como los llevables (por ejemplo, gafas). En esta descripción y en las reivindicaciones, la expresión "dispositivo informático" se define de manera amplia como que incluye cualquier dispositivo o sistema (o combinación de los mismos) que incluye al menos un procesador físico y tangible, y una memoria física y tangible que puede tener en la misma instrucciones ejecutables por ordenador que pueden ejecutarse por un procesador. La memoria puede tomar cualquier forma y puede depender de la naturaleza y forma del sistema informático. Un sistema informático puede distribuirse a través de un entorno de red y puede incluir múltiples sistemas informáticos constituyentes.

Como se ilustra en la Figura 1, en su configuración más básica, un sistema 100 informático típicamente incluye al menos una unidad 102 de procesamiento de hardware y la memoria 104. La memoria 104 puede ser memoria de sistema física, que puede ser volátil, no volátil o alguna combinación de las dos. El término "memoria" puede usarse también en el presente documento para hacer referencia a almacenamiento masivo no volátil tal como medio de almacenamiento físico. Si el sistema informático es distribuido, la capacidad de procesamiento, memoria y/o almacenamiento pueden también estar distribuidos. Como se usa en el presente documento, la expresión "módulo ejecutable" o "componente ejecutable" puede hacer referencia a objetos de software, rutinas, o procedimientos que pueden ejecutarse en el sistema informático. Los diferentes componentes, módulos, motores, y servicios descritos en el presente documento pueden implementarse como objetos o procedimientos que se ejecutan en el sistema informático (por ejemplo, como hilos separados).

En la descripción que sigue, se describen realizaciones con referencia a actos que se realizan por uno o más sistemas informáticos. Si tales actos se implementan en software, uno o más procesadores (del sistema informático asociado que realiza el acto) dirigen la operación del sistema informático en respuesta a haber ejecutado instrucciones ejecutables por ordenador. Por ejemplo, tales instrucciones ejecutables por ordenador pueden incorporarse en uno o más medios legibles por ordenador que forman un producto de programa informático. Un ejemplo de una operación de este tipo implica la manipulación de datos. Las instrucciones ejecutables por ordenador (y los datos manipulados) pueden almacenarse en la memoria 104 del sistema 100 informático. El sistema 100 informático puede contener también canales 108 de comunicación que permiten que el sistema 100 informático comunique con otros sistemas informáticos a través de, por ejemplo, la red 110. El sistema 100 informático también incluye una pantalla, que puede usarse para visualizar representaciones visuales para un usuario.

Las realizaciones descritas en el presente documento pueden comprender o utilizar un sistema informático de fin especial o de fin general que incluye hardware informático, tal como, por ejemplo, uno o más procesadores y memoria de sistema, como se analizan en mayor detalle a continuación. Las realizaciones descritas en el presente documento también incluyen medios físicos y otros legibles por ordenador para llevar a cabo o almacenar instrucciones ejecutables por ordenador y/o estructuras de datos. Tales medios legibles por ordenador pueden ser cualquier medio disponible que pueda accederse por un sistema informático de fin general o de fin especial. Medios legibles por ordenador que almacenan instrucciones ejecutables por ordenador son medios de almacenamiento físico. Medios legibles por ordenador que llevan instrucciones ejecutables por ordenador son medios de transmisión. Por lo tanto, a modo de ejemplo, y no como limitación, las realizaciones de la invención pueden comprender al menos dos clases diferentes de manera distinta de medios legibles por ordenador: medios de almacenamiento y medios de transmisión.

Medios de almacenamiento legible por ordenador incluyen RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier

otro medio de almacenamiento físico y tangible que puede usarse para almacenar medios de código de programa deseado en forma de instrucciones ejecutables por ordenador o estructuras de datos y que puede accederse por un sistema informático de fin general o de fin especial.

Una "red" se define como uno o más enlaces de datos que posibilitan el transporte de datos electrónicos entre sistemas informáticos y/o módulos y/u otros dispositivos electrónicos. Cuando se transfiere o proporciona información a través de una red u otra conexión de comunicaciones (ya sea de cableado permanente, inalámbrica, o una combinación de cableado permanente o inalámbrica) a un sistema informático, el sistema informático visualiza de manera apropiada la conexión como un medio de transmisión. Medio de transmisión puede incluir una red y/o enlaces de datos que pueden usarse para llevar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y que puede accederse por un sistema informático de fin general o de fin especial. Se deberían incluir también combinaciones de lo anterior dentro del ámbito de los medios legibles por ordenador.

Además, tras alcanzar diversos componentes de sistema informáticos, los medios de código de programa en forma de instrucciones ejecutables por ordenador o estructuras de datos pueden transferirse automáticamente desde los medios de transmisión a los medios de almacenamiento (o viceversa). Por ejemplo, las instrucciones ejecutables por ordenador o estructuras de datos recibidas a través de una red o enlace de datos pueden almacenarse en memoria intermedia en RAM en un módulo de interfaz de red (por ejemplo, un "NIC"), y a continuación transferirse eventualmente a la RAM de sistema informático y/o a medios de almacenamiento menos volátiles en un sistema informático. Por lo tanto, debería entenderse que los medios de almacenamiento pueden incluirse en componentes de sistema informáticos que también (o incluso principalmente) utilizan medios de transmisión.

Instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que, cuando se ejecutan en un procesador, provocan que un sistema informático de fin general, sistema informático de fin especial, o dispositivo de procesamiento de fin especial realicen una cierta función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, binarios o incluso instrucciones que experimentan alguna traducción (tal como compilación) antes de la ejecución directa por el procesador, tal como instrucciones de formato intermedio tal como lenguaje ensamblador, o incluso código fuente. Aunque se ha descrito la materia objeto en lenguaje específico a características estructurales y/o actos metodológicos, se ha de entender que la materia objeto definida en las reivindicaciones adjuntas no está necesariamente limitada a las características o actos anteriormente descritos. En su lugar, las características y actos descritos se desvelan como formas de ejemplo de implementación de las reivindicaciones.

Los expertos en la materia apreciarán que la invención puede ponerse en práctica en entornos informáticos de red con muchos tipos de configuraciones de sistema informático, incluyendo, ordenadores personales, ordenadores de sobremesa, ordenadores portátiles, procesadores de mensajes, dispositivos portátiles, sistemas multiprocesador, electrónica de consumo basada en microprocesador o programable, PC de red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, buscapersonas, encaminadores, conmutadores, centros de datos, llevables (tales como gafas) y similares. La invención puede ponerse en práctica también en entornos de sistema distribuidos donde los sistemas informáticos locales y remotos, que están enlazados (ya sea por enlaces de datos de cableado permanente, enlaces de datos inalámbricos, o por una combinación de enlaces de datos de cableado permanente e inalámbricos) a través de una red, ambos realizan tareas. En un entorno de sistema distribuido, los módulos de programa pueden localizarse tanto en dispositivos de almacenamiento de memoria locales como remotos.

La Figura 2 ilustra un sistema 200 que incluye un sistema 201 solicitante y un sistema 202 de origen. En particular, el sistema 201 solicitante envía una solicitud 231 al sistema 202 de origen para realizar una operación en una entidad de sistema de ficheros del sistema 202 de origen. Ejemplos de tales operaciones pueden incluir, por ejemplo, operaciones de lectura, operaciones de actualización, opciones de copia y opciones de borrado. La entidad de sistema de ficheros puede ser, por ejemplo, un disco, una partición, un directorio, o la entidad de sistema de ficheros más básica - un fichero.

El sistema 201 solicitante puede ser un sistema informático, caso en el que el sistema 201 solicitante puede estar estructurado como se ha descrito anteriormente para el sistema 100 informático de la Figura 1. Si es un sistema informático, el sistema 201 solicitante opera en el mismo un sistema 210 operativo. El sistema 202 de origen incluye un sistema 220 operativo que mantiene un sistema 221 de ficheros que constituye múltiples entidades 222 de sistema de ficheros. Por ejemplo, el sistema 221 de ficheros se ilustra como que incluye múltiples entidades 222 de sistema de ficheros que incluyen la entidad 222A de sistema de ficheros, la entidad 222B de sistema de ficheros, la entidad 222C de sistema de ficheros, entre potencialmente muchas otras entidades de sistema de ficheros como se representa por las elipses 222D. El sistema 202 de origen puede estructurarse análogamente como se ha descrito anteriormente para el sistema 100 informático de la Figura 1.

La Figura 3 ilustra un entorno 300 de entidad de sistema de ficheros. El entorno 300 de entidad de sistema de ficheros incluye una entidad 301 de sistema de ficheros así como datos 302 de localización y datos 303 de caducidad de operación. Adicionalmente, los datos 302 de localización y los datos 303 de caducidad de operación están asociados con la entidad 301 de sistema de ficheros como se representa por el recuadro 304 de línea discontinua. Esta asociación 304 es de manera que la entidad 301 de sistema de ficheros, los datos 302 de

localización y los datos 303 de caducidad de operación se mueven o copian de manera atómica juntos. Como un ejemplo, la entidad 301 de sistema de ficheros puede ser cualquiera de las entidades 222 del sistema de ficheros de la Figura 2. Un entorno 300 de entidad de sistema de ficheros similar puede proporcionarse para cada una de múltiples entidades de sistema de ficheros, de manera que la entidad de sistema de ficheros tiene datos de localización y datos de caducidad de operación asociados que se mueven o copian de manera atómica con la entidad de sistema de ficheros si la entidad de sistema de ficheros se mueve o copia, respectivamente.

La asociación 304 puede diferir dependiendo del sistema de ficheros. En un ejemplo, en el que la entidad de sistema de ficheros es un fichero, la asociación 304 se consigue incluyendo los datos de localización y datos de caducidad de operación en un flujo de datos del fichero alternativo. Esto puede ser apropiado por ejemplo, en un sistema de ficheros basado en el Sistema de Ficheros de Nueva Tecnología (NTFS). Como otro ejemplo, la asociación 304 puede conseguirse incluyendo los datos de localización y datos de caducidad de operación como una o más propiedades de la entidad de sistema de ficheros. Por ejemplo, en sistemas de ficheros basados en inodos tales como XFS, ZFS y Reiser4, estos datos de localización y datos de caducidad de operación pueden almacenarse contra un fichero que usa propiedades de fichero extendidas.

Para sistemas de ficheros que no proporcionan una extensión a un contenido de la entrada de la entidad del sistema de ficheros dado (tal como FAT16, FAT32 y ExFAT), puede usarse un enfoque de repliegue donde los datos de localización y los datos de caducidad de operación se escriben en un fichero separado en el mismo directorio que la entidad de sistema de ficheros (por ejemplo, usando una extensión apropiada). Aunque este no es tan robusto como los otros enfoques, ofrece algún nivel de interoperabilidad para sistemas heredados - aunque la aplicación del acceso de datos basada en localización y la aplicación de acceso basada en caducidad de operación estarán a merced del sistema operativo del consumidor.

No es importante para los principios descritos en el presente documento cómo se hace la asociación 304 entre la entidad 301 de sistema de ficheros y los datos 302 de localización y los datos 303 de caducidad de operación. Es suficiente decir que independientemente de cómo se haga la asociación, la asociación es compatible con el sistema de ficheros o entornos subyacentes, y se hace de manera que si la entidad 301 de sistema de ficheros se mueve o copia, también lo hacen los datos 302 de localización y los datos 303 de caducidad de operación.

La Figura 4 ilustra datos 400 complementarios que representan los datos 302 de localización y los datos 303 de caducidad de operación de la Figura 3. Los datos 400 complementarios incluyen diversos campos que son ejemplos de lo que puede incluirse en diversas realizaciones. No hay requisito entonces de que los datos 302 de localización o los datos 303 de caducidad de operación descritos en el presente documento incluyan todos, o incluso algunos, de los campos descritos para los datos 400 complementarios.

Los datos 400 complementarios incluyen una firma 401 que tal vez permita que se identifiquen los metadatos como que pertenecen a acceso de tiempo restringido. Un campo 402 de versión puede identificar el número de versión para permitir el avance de los principios descritos en el presente documento. Un campo 403 de origen de localización puede identificar una región en la que se originó la entidad de sistema de ficheros. Esto puede ser útil en situaciones en las que la caducidad de acceso o de operación puede depender de si la localización del solicitante es el mismo territorio que el que originó la entidad de sistema de ficheros.

Los datos 400 complementarios también incluyen un campo 410 de tiempo de vida de entidad que, si está presente, puede usarse para definir un tiempo de vida de la misma entidad de sistema de ficheros, independientemente del estado de localización del solicitante. En un ejemplo, el campo 410 de tiempo de vida puede incluir un campo 411 de caducidad de fichero y un indicador 412 de borrado. Por ejemplo, el campo 411 de caducidad de fichero puede ser un entero sin signo, y el indicador 412 de borrado puede ser un booleano.

Cuando se evalúa, como un ejemplo únicamente, un valor negativo en el entero grande 411 con signo indica que la correspondiente entidad de sistema de ficheros ya ha caducado, y es únicamente elegible para operaciones de borrado. El booleano 412 representa si la entidad de sistema de ficheros se ha de borrar o no automáticamente si la entidad de sistema de ficheros se halla que ha caducado. En este ejemplo, un valor cero en el entero grande 411 con signo indica que la entidad de sistema de ficheros actualmente no tiene un tiempo de caducidad. Un valor positivo en el entero grande 411 con signo indica un tiempo de caducidad, que puede compararse con el tiempo actual, para determinar si la entidad de sistema de ficheros ha caducado o no. De nuevo, si el entero grande 411 con signo se usa para indicar que la entidad de sistema de ficheros ha caducado, el booleano 412 se evalúa para determinar si la entidad de sistema de ficheros se ha de borrar o no automáticamente tras la detección de que la entidad de sistema de ficheros ha caducado.

Los datos 400 complementarios también incluyen un campo 420 de caducidad de territorio. En un ejemplo, al menos uno de (y potencialmente ambos) el campo 410 de fichero de tiempo de vida y el campo 420 de caducidad de territorio han de existir en los datos 400 complementarios. El campo 420 de caducidad de territorio incluye múltiples campos de territorio, cada uno para un correspondiente territorio. Por ejemplo, el campo 420 de caducidad de territorio se ilustra como que incluye tres campos 421, 422 y 423 de territorios. Sin embargo, las elipses 424 representan simbólicamente que puede haber cualquier número de campos de territorio en el campo 420 de caducidad de territorio. Como un ejemplo, cada campo de territorio (421 a 424) puede identificar el correspondiente

país usando cualesquiera medios. Ejemplos de tales identidades pueden incluir un código de país de las Naciones Unidas. En una realización, uno del campo de territorio es un campo de territorio por defecto que se aplica si el estado de localización de los solicitantes es desconocido o no está presente en ninguno de los otros territorios para los que hay un campo de territorio.

La Figura 5 ilustra de manera abstracta un campo 500 de territorio que representa un ejemplo de cualquiera de los campos 421 a 424 de territorio de la Figura 4. El campo 500 de territorio incluye múltiples campos de operación. En particular, el campo 500 de territorio se ilustra como que incluye cuatro campos 510, 520, 530 y 540 de operación. Sin embargo, las elipses 550 representan que puede haber cualquier número de campos de operación en el campo de territorio. Ejemplos de operaciones pueden incluir leer, copiar, actualizar y borrar. Cada campo 510, 520, 530 y 540 de caducidad de operación incluye un respectivo campo 511, 521, 531 y 541 de indicador de caducidad de operación, respectivamente, y un campo 512, 522, 532 y 542 de indicador de borrado, respectivamente. Si viene una solicitud en la que indica que el solicitante tiene un estado de localización que corresponde a uno de los territorios representados en el campo 420 de caducidad de territorio, entonces se identifica la operación solicitada para determinar qué campo de caducidad de operación del respectivo campo de territorio (por ejemplo, 421 y 500) usar para definir si se permite la operación, o ya no se permite. De nuevo, en una realización, cada campo 511, 521, 531 y 541 de indicador de caducidad de operación puede ser un entero grande sin signo, y cada campo 512, 522, 532 y 542 de indicador de borrado puede ser un booleano.

Cuando se evalúa, un valor negativo en el entero grande con signo para el respectivo campo 510, 520, 530, 540 de indicador de caducidad de operación indica que la operación para la correspondiente entidad de sistema de ficheros ya ha caducado dado el estado de la localización del solicitante, y es únicamente elegible para operaciones de borrado si se permite dado el estado de la localización del solicitante. El booleano representa si la entidad de sistema de ficheros se ha de borrar o no automáticamente si la entidad de sistema de ficheros se halla que ha caducado. En este ejemplo, un valor cero en el entero grande con signo indica que la respectiva operación en la respectiva entidad de sistema de ficheros actualmente no tiene un tiempo de caducidad dado el estado de la localización del solicitante. Un valor positivo en el entero grande con signo indica un tiempo de caducidad que puede compararse con el tiempo actual para determinar si la respectiva operación para la entidad de sistema de ficheros ha expirado o no dada la localización del solicitante. De nuevo, si el entero grande con signo se usa para indicar que la operación en la entidad de sistema de ficheros ha caducado dada la localización del solicitante, el booleano se evalúa para determinar si la entidad de sistema de ficheros se ha de borrar o no automáticamente.

La Figura 6 ilustra un diagrama de flujo de un procedimiento 600 para controlar el acceso a datos basándose en la localización del solicitante y datos de caducidad. El procedimiento 600 puede realizarse por, por ejemplo, el sistema 202 de origen para controlar el acceso a una o más de las entidades 222 del sistema de ficheros en su sistema 221 de ficheros. Por consiguiente, el procedimiento 600 puede describirse con referencia frecuente a la Figura 2 como un ejemplo.

El procedimiento 600 se inicia después de que el sistema de origen reciba una solicitud para realizar una operación en la entidad de sistema de ficheros (acto 601). Por ejemplo, en la Figura 2, el sistema 202 de origen recibe la solicitud 231 desde el sistema 201 solicitante. Por ejemplo, supóngase que la solicitud 231 es para realizar una operación de lectura en la entidad 222A de sistema de ficheros.

El sistema de origen a continuación identifica un estado de localización asociado con el solicitante que emite la solicitud (acto 602). Por ejemplo, en la Figura 2, el sistema 202 de origen determinaría el estado de localización de la entidad 201 solicitante. El estado de localización puede ser "desconocido" en casos en los que la localización del solicitante no puede determinarse. El estado de localización puede ser también una localización o territorio particular donde el solicitante está actualmente localizado.

A continuación, el sistema de origen identifica datos de caducidad (acto 603) que corresponden al estado de localización, y que está asociado con la operación solicitada. Por ejemplo, haciendo referencia a la Figura 2, supóngase que la entidad 222A de sistema de ficheros se solicita para que se opere, y que la entidad 222A de sistema de ficheros incluye un entorno 300 de entidad de sistema de ficheros de la Figura 3. En ese caso, puede accederse (por ejemplo, deshacer la conversión a serie) a los datos complementarios apropiados (representados como los datos 400 complementarios de la Figura 4). Dado el estado de localización, puede localizarse el campo de territorio apropiado (por ejemplo, 421, 422, 423) de los datos 400 complementarios. Adicionalmente, dada la operación solicitada, se localiza el campo de operación apropiado (por ejemplo, 510, 520, 530 o 540 si se aplica el campo 500 de territorio).

Los datos de caducidad identificados se usan a continuación para determinar si la operación solicitada está permitida en la entidad de sistema de ficheros (bloque 604 de decisión). Por ejemplo, como se ha indicado anteriormente, si ("No" en el bloque 604 de decisión) el entero grande sin signo (por ejemplo, el campo 511) del campo de operación (por ejemplo, el campo 510) es negativo o el tiempo actual es posterior al tiempo representado en el campo de operación, entonces se deniega la operación solicitada (acto 605). Por ejemplo, esto puede implicar que el sistema de origen evite la operación en la entidad de sistema de ficheros. Por otra parte ("Sí" en el bloque 604 de decisión), si el entero grande 511 sin signo del campo de operación 510 es cero o el tiempo actual es anterior al tiempo representado en el campo de caducidad de operación, entonces se permite la operación solicitada (acto 606).

Si se deniega la operación ("No" en el bloque 604 de decisión), se usa el campo de borrado tras caducidad (por ejemplo, 512) del campo de operación (por ejemplo, 510) para determinar si la entidad de sistema de ficheros se ha de borrar automáticamente (bloque 607 de decisión). En caso afirmativo ("Sí" en el bloque 607 de decisión), se borra la entidad de sistema de ficheros (acto 610). De otra manera, el procedimiento finaliza (acto 609) para la operación solicitada. La entidad de sistema de ficheros permanece, pero, sin embargo, la solicitud para operar en la misma se ha denegado.

En el caso de que la operación solicitada se permita ("Sí" en el bloque 604 de decisión), el procedimiento 600 puede incluir adicionalmente provocar que se realice la operación solicitada en la entidad de sistema de ficheros. El sistema de origen puede a continuación determinar si la entidad de sistema de ficheros debería transcodificarse o no para que fuera compatible con el sistema 210 operativo del sistema 201 solicitante (bloque 611 de decisión). En el caso de que la operación del sistema de ficheros sea una operación de borrado, lectura o actualización, tal vez no sea necesaria la transcodificación ("No" en el bloque 611 de decisión), y el procedimiento finaliza (acto 609).

Sin embargo, en el caso de una operación de copia ("Sí" en el bloque 611 de decisión), la versión copiada de la entidad de sistema de ficheros puede transcodificarse (acto 612), dependiendo de si el entorno 300 de entidad de sistema de ficheros es el mismo entre los sistemas 210 y 220 de operación. Si no son iguales, a continuación se realiza la transcodificación por lo que entonces los datos 302 de localización, los datos 303 de caducidad de operación (es decir, los datos 400 complementarios) y la entidad 301 de sistema de ficheros están asociados 304 de una manera adecuada para el sistema 210 operativo de la entidad solicitante, o para el sistema operativo final en el que el solicitante va a usar la entidad de sistema de ficheros. Por ejemplo, la copia de la entidad de sistema de ficheros puede tener los datos complementarios copiados desde un flujo de datos alternativo (si no se reconoce por el sistema 210 operativo) a una propiedad de fichero. Además, pueden cambiarse formatos de conversión a serie. Si la entidad de sistema de ficheros se convierte a serie de una manera que en el sistema 220 operativo de origen no se reconoce por el sistema 210 operativo solicitante (o el sistema operativo en el que el solicitante pretende usar la entidad de sistema de ficheros), entonces puede realizarse la transcodificación en la forma o la reconversión a serie.

La Figura 7 ilustra un procedimiento 700 más específico para controlar el acceso a una entidad de sistema de ficheros basándose en el estado de localización del solicitante y basándose en datos de caducidad específicos de operación. Tras recibir la solicitud (acto 701), se inicia el procedimiento 700. Se accede a continuación (acto 702) a los datos 400 complementarios (denominados en la Figura 7 como "metadatos (M) de tiempo y localización") para la correspondiente entidad de sistema de ficheros. Esto puede implicar deshacer la conversión a serie de los datos 400 complementarios.

El estado de localización del solicitante se determina a continuación (acto 703). El acto 703 es un ejemplo del acto 602 de la Figura 6. El estado de localización puede ser "desconocido" en el caso en el que la localización del solicitante no pueda determinarse.

Se determina a continuación si hay o no algún dato de tiempo de vida de la entidad (por ejemplo, el campo 410 se rellena de manera válida) en los datos 400 complementarios (acto 704). Si hay ("Sí" en el bloque 704 de decisión), el procedimiento 700 participa en los actos 705 a 715 (algunos de los cuales son condicionales), que no se han descrito anteriormente con respecto a la Figura 6.

Específicamente, si el entero grande con signo para los datos de tiempo de vida de entidad es igual a cero ("Sí" en el bloque 705 de decisión)), esto significa que la entidad de sistema de ficheros nunca caduca, y por lo tanto se permite la operación (acto 706). Por otra parte ("No" en el bloque 705 de decisión), si el entero grande con signo es negativo ("Sí" en el bloque de decisión 707), entonces se determina que la entidad de sistema de ficheros ya ha caducado (acto 708). En ese caso, se evalúa el indicador 412 de borrado de fichero (bloque 709 de decisión). Si ese booleano es verdadero ("Sí" en el bloque 709 de decisión), entonces se borra la entidad de sistema de ficheros del disco (acto 710), y se aborta la operación (acto 711). De otra manera, si el booleano es falso ("No" en el bloque 709 de decisión), entonces se aborta la operación (acto 711) sin borrar la entidad de sistema de ficheros (omitiendo el acto 710).

Si el entero grande con signo no es cero ("No" en el bloque 705 de decisión), y no es negativo ("No" en el bloque de decisión 707), entonces se evalúa el entero grande con signo como una indicación de fecha/hora (acto 712). Un ejemplo de una indicación de fecha/hora es una indicación de fecha/hora de Unix. Si el tiempo actual es mayor que la indicación de fecha/hora ("Sí" en el bloque de decisión 713), a continuación se determina que el fichero de nuevo ha caducado (acto 714), y de nuevo se evalúa el indicador 412 de borrado (bloque 709 de decisión). De nuevo, si se establece el indicador 412 de borrado de fichero ("Sí" en el bloque 709 de decisión), entonces se borra la entidad de sistema de ficheros (acto 710) y se aborta la operación solicitada (acto 711). Si no se establece el indicador 412 de borrado ("No" en el bloque 709 de decisión), entonces se aborta la operación solicitada (acto 711) sin borrar la entidad de sistema de ficheros. Si el entero grande con signo es positivo ("No" en los bloques 705 y 707 de decisión), y el tiempo actual es menor que la indicación de fecha/hora ("No" en el bloque de decisión 715), entonces se permite que la operación solicitada continúe (acto 715).

Volviendo al bloque 704 de decisión, si los datos complementarios no incluyen un campo 410 de tiempo de vida de entidad rellenado ("No" en el bloque 704 de decisión), entonces se determina (bloque 716 de decisión) si el estado

de localización del solicitante es desconocido o de lo contrario no está en la lista de territorios en el campo 420 de territorio ("No" en el bloque 716 de decisión). En ese caso, se usa un conjunto de reglas de caducidad por defecto para la operación (acto 717) (un "conjunto de reglas de caducidad" de la Figura 7 corresponde a un campo de territorio (por ejemplo, 421 a 424) de la Figura 4). Por ejemplo, en una realización, el campo 421 de territorio puede usarse en el caso en el que el territorio del solicitante sea desconocido o no esté en los otros territorios enumerados. Si la localización del solicitante es una localización particular que corresponde a un territorio real que corresponde a los campos de territorio ("Sí" en el bloque 716 de decisión), entonces se usa el conjunto de reglas de caducidad para el territorio específico (acto 718). Por ejemplo, tal vez el campo 421 de territorio corresponde a un estado de localización desconocido (es decir, es un conjunto de reglas por defecto), mientras que el campo 422 de territorio puede corresponder al Reino Unido. En ese caso, si el solicitante determina que está localizado en el Reino Unido, entonces se usaría el campo 422 de territorio.

En cualquier caso, si a través de un conjunto de reglas por defecto (acto 717) o a través del uso de un conjunto de reglas de territorio (acto 718), se obtiene un conjunto de reglas, y se obtiene el campo de caducidad de operación pertinente. Por ejemplo, si la operación solicitada fuera una operación de copia, y el campo 510 de operación fuera para una operación de copia. Se accedería al campo 511 de indicador de caducidad de operación, y se evaluaría (acto 719). Esto correspondería al acto 603 de la Figura 6.

Específicamente, si el entero grande con signo para el campo de indicador de caducidad de operación es igual a cero ("Sí" en el bloque 720 de decisión), esto significa que la operación de la entidad de sistema de ficheros nunca caduca (determinación 721) dado el estado de localización del solicitante, y por lo tanto se permite la operación. Por otra parte ("No" en el bloque 720 de decisión), si el entero grande con signo es negativo ("Sí" en el bloque 722 de decisión), entonces se determina que la operación en la entidad de sistema de ficheros ya ha caducado (acto 723) dado el estado de localización del solicitante. En ese caso, se evalúa (bloque 724 de decisión) el campo de indicador de borrado (por ejemplo, 512 para el campo 510 de operación). Si ese booleano es verdadero ("Sí" en el bloque 724 de decisión), entonces se borra la entidad de sistema de ficheros del disco (acto 725), y se aborta la operación (acto 726). De otra manera, si el booleano es falso ("No" en el bloque 724 de decisión), entonces se aborta la operación (acto 726) sin borrar la entidad de sistema de ficheros (omitiendo el acto 725).

Si el entero grande con signo no es cero ("No" en el bloque 720 de decisión), y no es negativo ("No" en el bloque de decisión 722), entonces se evalúa el entero grande con signo como una indicación de fecha/hora (acto 727). De nuevo, un ejemplo de una indicación de fecha/hora es una indicación de fecha/hora de Unix. Si el tiempo actual es mayor que la indicación de fecha/hora ("Sí" en el bloque 728 de decisión), entonces se determina de nuevo que la operación en la entidad de sistema de ficheros ha caducado (acto 729), y de nuevo se evalúa (bloque 724 de decisión) el campo 512 de indicador de borrado. De nuevo, si se establece el indicador 412 de borrado ("Sí" en el bloque 724 de decisión), entonces se borra la entidad de sistema de ficheros (acto 725) y se aborta la operación solicitada (acto 726). Si no se establece el campo 512 de indicador de borrado ("No" en el bloque 724 de decisión), entonces se aborta la operación solicitada (acto 726) sin borrar la entidad de sistema de ficheros. Si el entero grande con signo es positivo ("No" en los bloques 720 y 722 de decisión), y el tiempo actual es menor que la indicación de fecha/hora ("No" en el bloque 728 de decisión), entonces se permite que continúe la operación solicitada (acto 730).

Los principios descritos en el presente documento permiten por lo tanto que se cumpla la soberanía de datos y los datos de caducidad a la granularidad de una única operación de manera que las operaciones (y sus caducidades) en las entidades de sistema de ficheros (por ejemplo, ficheros) pueden limitarse por la localización del solicitante. Adicionalmente, cuando se permite la operación, y ha de hacerse disponible una copia del sistema de ficheros, el entorno de entidad de sistema de ficheros puede transcodificarse de manera que el sistema solicitante puede tener acceso también a los datos de localización y a los datos de caducidad de operación, haciendo cumplir de esta manera las reglas de soberanía de datos con respecto a acceso y caducidad.

Habiendo descrito una estructura de ejemplo de los datos complementarios con respecto a la Figura 4, se describirán ahora tres implementaciones de conversión a serie específicas con respecto a las Tablas 1A a 3 respectivamente. Las Tablas 1A y 1B a continuación ilustran un formato de fichero binario para los datos de localización. La Tabla 1A ilustra un formato de encabezamiento de fichero de ejemplo. La Tabla 1B ilustra estructuras de datos de soporte de ejemplo.

Encabezamiento de fichero

TABLA 1A

Sección	*Tipo de datos*	*Valor*	*Notas*
Firma	*4 * bytes*	*TIEMPO*	*Número de fichero mágico para identificar este formato de fichero de metadatos*
Información de versión	*int*	*10*	*A leerse en la forma x.y (10 indica versión 1.0)*

(continuación)

Sección	*Tipo de datos*	*Valor*	*Notas*
¿Usar TTL absoluto?	*Booleano*	*-*	*Este valor determina si usar comportamiento de tiempo de vida absoluto (verdadero) o un conjunto de reglas específicas de territorio (falso)*
Recuento de territorio	*int*	*n*	*El número total de reglas de caducidad de operación de fichero específicas de territorio. Si el campo anterior es 'verdadero', entonces este número será '0'*
[Tiempo de vida absoluto]	*ttl_struct*		*Únicamente presente si 'Usar TTL absoluto' equivale a 'verdadero'*
*[Conjunto de reglas de territorio] * n*	*geo_struct*		*Si 'Usar TTL absoluto' equivale a 'falso', entonces habrá una geo_struct para cada conjunto de reglas territoriales definidas (hasta el máximo definido 'Recuento de territorio')*
[Conjunto de reglas por defecto]	*def_struct*		*Si 'Usar TTL Absoluto' equivale a falso', habrá una def_struct para representar el conjunto de reglas por defecto para usar si un territorio no se define en la colección anterior de geo_struct*

Soportar tipos de datos

TABLA 1B

Nombre de tipo	*Nombre de campo*	*Tipo de datos*	*Notas*
ttl_struct			*Si está presente, este determina un tiempo de vida absoluto del fichero*
ttl_struct	*Indicación de tiempo*	*entero grande con signo*	*Un valor negativo indica que un fichero ya ha caducado. Un valor cero indica que un fichero nunca caducará. Un número positivo representa una indicación de fecha/hora de unix. Una vez que esta indicación de fecha/hora ha pasado, este fichero ya no será elegible para cualquier operación de fichero distinta de borrado.*
ttl_struct	*Borrar al caducar*	*bool*	*Esto determina si el sistema operativo debería borrar físicamente el fichero del disco (sin ningún almacén de datos de recuperación intermediario - por ejemplo. La papelera de reciclaje)*
geo_struct			*Si está presente, este representa un conjunto de reglas de caducidad de operación que se aplican a un territorio específico*
geo_struct	*Territorio*	*int*	*Hace referencia a un código de país numérico UN (Por ejemplo, 826 es el Reino Unido), usado para proporcionar contexto territorial para las reglas de caducidad de operación de fichero en esta estructura*
geo_struct	*Borrar al caducar*	*bool*	*Esto determina si el sistema operativo debería borrar físicamente el fichero del disco si una operación dada caduca*
geo_struct	*Caducidad de copia*	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de fecha/hora de unix que representa el plazo después de que ya no se permiten las operaciones de copia en este territorio.*
geo_struct	*Caducidad de lectura*	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de hora/fecha de unix que representa el plazo después del que ya no se permiten operaciones de lectura en este territorio.*

(continuación)

Nombre de tipo	*Nombre de campo*	*Tipo de datos*	*Notas*
geo_struct	*Caducidad de actualización*	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de hora/fecha de unix que representa el plazo después del cual ya no se permiten operaciones de actualización en este territorio. Las operaciones de actualización incluyen cambios a las indicaciones de tiempo, propiedad, metadatos y contenido.*
geo_struct	*Caducidad de borrado*	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de hora/fecha de unix que representa el plazo después del cual ya no se permiten operaciones de borrado en este territorio*
def_struct			*Este representa el conjunto de reglas de caducidad de operación de fichero por defecto para usar si no puede hallarse un conjunto de reglas territoriales específicas*
def_struct	*Borrar al caducar*	*bool*	*Esto determina si el sistema operativo debería borrar físicamente el fichero del disco si una operación dada caduca*
def_struct	*Caducidad de copia*	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de fecha/hora de unix que representa el plazo después de que ya no se permiten las operaciones de copia en este territorio.*
def_struct	*Caducidad de lectura*	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de hora/fecha de unix que representa el plazo después del que ya no se permiten operaciones de lectura en este territorio.*
def_struct	Caducidad de actualización	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de hora/fecha de unix que representa el plazo después del cual ya no se permiten operaciones de actualización en este territorio. Las operaciones de actualización incluyen cambios a las indicaciones de tiempo, propiedad, metadatos y contenido.*
def_struct	*Caducidad de borrado*	*entero grande con signo*	*Un valor negativo indica que esta operación no puede tener lugar nunca. Un valor cero indica que esta operación no puede caducar nunca. Un valor positivo es una indicación de hora/fecha de unix que representa el plazo después del cual ya no se permiten operaciones de borrado en este territorio.*

La Tabla 2 ilustra una realización más portátil de los datos de localización que usan Notación de Objetos de JavaScript (JSON).

```
{
    "EXPIRY": {
        "version": 1.0,                 // Este fichero debe contener uno de los [Opcionales] elementos a continuación para que sean válidos
        "origin": 826,                  // El país de origen para este fichero (código de país UN. 826 = UK)
        "TTL": {                        //[Opcional] Tiempo de vida absoluto
            "timestamp": "1420070400",  // Entero con signo que indica comportamiento de caducidad de fichero
                                        //-1 = Fichero ya ha caducado
                                        // 0 = Fichero nunca caduca
                                        // >0 = Indicación de tiempo de Unix para caducidad de fichero (en este // caso 01/01/2015)
```

```
"deleteOnExpiry": true      // Determina si borrar este fichero del
                            // sistema de ficheros tras la caducidad. El borrado NO debería
                            // usar almacenes de recuperación intermediarios },

"expiry": {                 //[Opcional] reglas de caducidad de operación específica de territorio

"geo_expiry": [             // Esto es una lista (serie) de territorios y sus
                            // reglas de caducidad de operación
                            // Únicamente se muestra una entrada de territorio por brevedad
{
"country": 784,             // El país al que esta regla específica aplica a (UN // código de país.
                             826 = UAE)
"deleteOnExpiry": true,     // Determina si borrar este fichero
                            //desde el sistema de ficheros tras la caducidad. El borrado
                            // NO debería usar almacenes de recuperación intermediarios
"copy": "-1 ",              // Entero con signo que rige la caducidad de operación de copia

"read": "1420070400",       //Número entero con signo que rige la caducidad de operación de lectura
"update": "-1",             //Número entero que rige la caducidad de operación de actualización

"delete": "0",              //Número entero con signo que rige la caducidad de operación de borrado

}
]
"default_expiry": {         // Este es el conjunto de reglas de caducidad de operación por defecto para
                            // usar si un conjunto de reglas territorial específicas no puede
                            //hallarse
"deleteOnExpiry": true,     // Determina si borrar este fichero
                            //desde el sistema de ficheros tras la caducidad. El borrado
                            // NO debería usar almacenes de recuperación intermediarios
"copy": "-1 ",              // Entero con signo que rige la operación de copia

"read": "1420070400",       //Número entero con signo que rige la caducidad de operación de lectura

"update": "-1 ",            //Número entero con signo que rige la operación de actualización

"delete": "0",              //Número entero con signo que rige la caducidad de operación de borrado
```

```
                    }
                  }
                }
              }
```

TABLA 2

La siguiente tabla 3 muestra un ejemplo portable de los datos de localización usando un documento de Lenguaje de Marcas Extensible (XML).

```
<?xml version="1.0" encoding="utf-8" ?>
<!-- Una versión basada en XML de los metadatos sensibles al tiempo -->
<!-- Un fichero debe contener uno de los nodos [Opcional] -->
<TimeMetadata>
<!-- Información de versión de metadatos -->
<Version>1.0</Version>
<!-- País de origen -->
<Origin>
   <IsoCode>UK</IsoCode>
   <UNCode>826</UNCode>
</Origin>
<!-- [Opcional] Tiempo de vida absoluto -->
<AbsoluteTimeToLive>
   <!-
      Un valor negativo indica que este fichero ya ha caducado.
      Un valor cero indica que este fichero nunca caducará.
      Un valor positivo indica una indicación de fecha/hora de unix,
      que representa la fecha y hora después de que ya no se permitirá
      el acceso al fichero.
   -->
   <TimeStamp>1420070400</TimeStamp>
   <!-- Determina si el fichero debería borrarse tras la caducidad -->
   <DeleteOnExpiry>true</DeleteOnExpiry>
</AbsoluteTimeToLive>
<!-- [Opcional] Reglas de caducidad de operación específica de territorio -->
<Expiry>
   <!-- La lista de territorios y sus conjuntos de reglas -->
   <GeoExpiry>
      <!-- Únicamente se muestra una entrada en este nivel por brevedad -->
      <Territory>
         <!-- Información territorial -->
         <IsoCode>ZWE</IsoCode>
         <UNCode>716</UNCode>
         <!-- Determina si borrar el fichero tras la caducidad de operación -->
         <DeleteOnExpiry>true</DeleteOnExpiry>
         <!-- Detalle de caducidad de operación para este territorio -->
         <Copy>-1</Copy>
         <Read>1420070400</Read>
         <Update>-1</Update>
         <Delete>0</Delete>
      </Territory>
   </GeoExpiry>
   <!-- El conjunto de reglas de caducidad por defecto para usar si no puede hallarse
   un territorio específico -->
   <Default>
      <!-- Determina si borrar el fichero tras la caducidad de operación -->
      <DeleteOnExpiry>true</DeleteOnExpiry>
      <!-- Caducidad de operación de fichero por defecto -->
      <Copy>-1</Copy>
      <Read>1420070400</Read>
      <Update>-1</Update>
      <Delete>0</Delete>
   </Default>
```

```
</Expiry>
</TimeMetadata>
```

TABLA 3

Por consiguiente, se ha descrito un mecanismo para conservar la soberanía de datos con caducidad aplicados por territorio y tiempo de vida específico de operación.

Sección de soporte de la reivindicación

En este punto se describe un procedimiento para controlar el acceso a una entidad de sistema de ficheros basándose en la localización del solicitante y datos de caducidad de operación del fichero. El procedimiento incluye un acto de asociar datos de caducidad de operación y datos de localización con una entidad de sistema de ficheros de manera que los datos de caducidad de operación y los datos de localización y la entidad de sistema de ficheros se mueven o copian de manera atómica juntos; un acto de recibir una solicitud para realizar una operación en la entidad de sistema de ficheros; un acto de identificar un estado de localización asociado con un solicitante de la solicitud; un acto de identificar datos de caducidad que corresponden al estado de localización, y que está asociado con la operación solicitada; y un acto de usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en la entidad de sistema de ficheros.

El acto de asociar los datos de día de caducidad de operación y de localización con la entidad de sistema de ficheros puede incluir un acto de incluir los datos de día de caducidad de operación y de localización en un flujo de datos alternativo de la entidad de sistema de ficheros. El acto de asociar datos de día de caducidad de operación y de localización con la entidad de sistema de ficheros comprende puede incluir un acto de incluir los datos de caducidad de operación y de localización como una o más propiedades de la entidad de sistema de ficheros.

El acto de usar los datos de caducidad identificados para determinar si la operación solicitada se permite o no puede comprender: un acto de determinar que el estado de localización del solicitante es desconocido; y en respuesta a la determinación que el estado de localización del solicitante es desconocido, un acto de acceder a un conjunto de reglas de caducidad por defecto para la operación solicitada; y un acto de determinar si la operación solicitada puede realizarse o no basándose en el conjunto de reglas por defecto. Cuando el estado de localización del solicitante es una localización del solicitante, los datos de caducidad identificados pueden incluirse en los datos de caducidad de operación asociados para la entidad de sistema de ficheros.

El acto de usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en la entidad de sistema de ficheros puede comprender: un acto de determinar un tiempo de caducidad en los datos de caducidad identificados; un acto de determinar un tiempo pertinente para comparar al tiempo de caducidad; y un acto de determinar si se determina si se permite la operación solicitada basándose en la comparación del tiempo pertinente al tiempo de caducidad.

El acto de usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en el sistema de ficheros puede comprender: un acto de interpretar los datos de caducidad como que indican que no hay caducidad para la operación solicitada; y un acto de permitir la operación basándose en la ausencia de caducidad para la operación solicitada.

El acto de usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en el sistema de ficheros puede comprender: un acto de interpretar los datos de caducidad como que indican que la operación solicitada ha caducado sin referencia a un tiempo de caducidad; y un acto de denegar la operación basándose en el estado caducado para la operación solicitada.

El procedimiento comprende adicionalmente lo siguiente si se determina que se permite la operación solicitada: un acto de provocar la operación solicitada para realizarse en la entidad de sistema de ficheros. En ese caso, el acto de provocar que la operación solicitada se realice puede comprender: un acto de transcodificar la entidad de sistema de ficheros para que sea una entidad de sistema de ficheros transcodificada que es adecuada para un sistema operativo del solicitante. Como alternativa o además, el acto de provocar que se realice la operación de entidad de sistema de ficheros solicitada puede comprender: un acto de transcodificar la entidad de sistema de ficheros para que sea en una implementación de conversión a serie que se implementa por un sistema operativo del solicitante.

También se describe en el presente documento un producto de programa informático que comprende uno o más medios de almacenamiento legibles por ordenador que tienen en el mismo una o más instrucciones ejecutables por ordenador que se estructuran de manera que, cuando se ejecutan por el uno o más procesadores del sistema informático, provocan que el sistema informático realice lo siguiente en respuesta a recibir una solicitud para realizar una operación en una entidad de sistema de ficheros que se gestiona por un sistema operativo, teniendo la entidad de sistema de ficheros datos de caducidad de operación y datos de localización asociados con la entidad de sistema de ficheros de manera que los datos de caducidad de operación y los datos de localización y la entidad de sistema de ficheros se mueven o copian de manera atómica juntos: un acto de identificar un estado de localización asociado con un solicitante de la solicitud; un acto de identificar datos de caducidad que corresponden al estado de localización, y que está asociado con la operación solicitada; y un acto de usar los datos de caducidad identificados

para determinar si la operación solicitada está permitida en la entidad de sistema de ficheros.

El producto de programa informático puede comprender adicionalmente instrucciones ejecutables por ordenador que se estructuran de manera que, cuando se ejecutan por el uno o más procesadores del sistema informático, provocan que el sistema informático realice lo siguiente: un acto de identificar si hay datos de caducidad de fichero asociados con la entidad de sistema de ficheros que es el objetivo de la prueba solicitada, en el que si los datos de caducidad de fichero están presentes, los datos de caducidad de fichero se usan para determinar si se permiten operaciones en el fichero. Si las operaciones en el fichero no se permiten por los datos de caducidad de fichero, se hace referencia a datos de borrado de fichero para determinar si borrar la entidad de sistema de ficheros, en el que si el borrado de fichero indica que la entidad de sistema de ficheros debería borrarse, se borra la entidad de sistema de ficheros.

También se describe en el presente documento un sistema informático que comprende: uno o más medios de almacenamiento legibles por ordenador que tienen en los mismos una pluralidad de entidades de sistema de ficheros gestionadas por un sistema operativo del sistema informático, al menos una entidad de sistema de ficheros particular de la pluralidad de ficheros que tiene datos de localización de datos de caducidad de operación asociados que está asociada con la entidad de sistema de ficheros particular de manera que los datos de caducidad de operación y los datos de localización y la entidad de sistema de ficheros particular se mueven o copian de manera atómica juntos; y uno o más procesadores. El uno o más medios legibles por ordenador pueden tener en los mismos instrucciones ejecutables por ordenador que están configuradas de manera que, cuando se ejecutan por el uno o más procesadores, provocan que el sistema informático realice lo siguiente en respuesta a recibir una solicitud para realizar una operación en la localización de sistema de ficheros particular: un acto de identificar una localización asociada con un solicitante de la solicitud; y un acto de usar los datos de localización para determinar si la operación de fichero solicitada está permitida o no en la entidad de sistema de ficheros particular.

La presente invención puede realizarse en otras formas específicas. Las realizaciones descritas se han de considerar en todos los aspectos únicamente como ilustrativas y no restrictivas. El alcance de la invención se indica, por lo tanto, por las reivindicaciones adjuntas en lugar de por la descripción anterior. Todos los cambios que entran dentro del significado y alcance de equivalencia de las reivindicaciones han de abarcarse dentro de su alcance.

REIVINDICACIONES

1. Un procedimiento implementado por ordenador para controlar el acceso a una entidad de sistema de ficheros basándose en la localización del solicitante y datos de caducidad de operación del fichero, realizándose el procedimiento implementado por ordenador por uno o más procesadores que ejecutan instrucciones ejecutables por ordenador para el procedimiento implementado por ordenador, y comprendiendo el procedimiento implementado por ordenador:

asociar datos de caducidad de operación y datos de localización con una entidad de sistema de ficheros de manera que los datos de caducidad de operación y los datos de localización y la entidad de sistema de ficheros se mueven o copian de manera atómica juntos;
recibir una solicitud para realizar una operación en la entidad de sistema de ficheros;
identificar un estado de localización asociado con un solicitante de la solicitud;
identificar datos de caducidad que corresponden al estado de localización, y que está asociado con la operación solicitada; y
usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en la entidad de sistema de ficheros; en el que, si se determina que la operación solicitada no está permitida, el procedimiento comprende adicionalmente:

determinar si la entidad de sistema de ficheros se ha de borrar automáticamente basándose en una entrada de un campo de indicador de borrado asociado con los datos de caducidad de operación; y en caso afirmativo, borrar automáticamente la entidad de sistema de ficheros.

2. El procedimiento implementado por ordenador de acuerdo con la reivindicación 1, en el que asociar datos de día de caducidad de operación y de localización con la entidad de sistema de ficheros comprende incluir los datos de día de caducidad de operación y de localización en un flujo de datos alternativo de la entidad de sistema de ficheros.

3. El procedimiento implementado por ordenador de acuerdo con la reivindicación 1, en el que asociar datos de día de caducidad de operación y de localización con la entidad de sistema de ficheros comprende incluir los datos de día de caducidad de operación y de localización como una o más propiedades de la entidad de sistema de ficheros.

4. El procedimiento implementado por ordenador de acuerdo con la reivindicación 1, en el que usar los datos de caducidad identificados para determinar si se permite o no la operación solicitada comprende:

determinar que el estado de localización del solicitante es desconocido;
en respuesta a la determinación de que el estado de localización del solicitante es desconocido, acceder a un conjunto de reglas de caducidad por defecto para la operación solicitada; y
determinar si la operación solicitada puede realizarse o no basándose en el conjunto de reglas por defecto.

5. El procedimiento implementado por ordenador de acuerdo con la reivindicación 1, en el que usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en la entidad de sistema de ficheros comprende:

determinar un tiempo de caducidad en los datos de caducidad identificados;
determinar un tiempo pertinente para comparar al tiempo de caducidad; y
determinar si se determina que se permite la operación solicitada basándose en la comparación del tiempo pertinente al tiempo de caducidad.

6. El procedimiento implementado por ordenador de acuerdo con la reivindicación 1, en el que usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en el sistema de ficheros comprende:

interpretar los datos de caducidad como que indican que no hay caducidad para la operación solicitada; y permitir la operación basándose en la ausencia de caducidad para la operación solicitada.

7. El procedimiento implementado por ordenador de acuerdo con la reivindicación 1, en el que usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en el sistema de ficheros comprende:

interpretar los datos de caducidad como que indican que la operación solicitada ha caducado sin referencia a un tiempo de caducidad; y
denegar la operación basándose en el estado caducado para la operación solicitada.

8. El procedimiento implementado por ordenador de acuerdo con la reivindicación 1, en el que, si se determina que se permite la operación solicitada, el procedimiento implementado por ordenador comprende adicionalmente provocar que la operación solicitada se realice en la entidad de sistema de ficheros.

9. Un sistema informático que comprende:

uno o más procesadores;
uno o más medios de almacenamiento legibles por ordenador que comprenden instrucciones ejecutables que, cuando se realizan por el uno o más procesadores, provocan que el sistema informático se configure con una arquitectura que comprende una pluralidad de entidades de sistema de ficheros gestionadas por un sistema operativo del sistema informático, al menos una entidad de sistema de ficheros particular de la pluralidad de ficheros que tiene datos de localización de datos de caducidad de operación asociados que están asociados con la entidad de sistema de ficheros particular, de manera que los datos de caducidad de operación y los datos de localización y la entidad de sistema de ficheros particular se mueven o copian de manera atómica conjuntamente; y
las instrucciones ejecutables por ordenador realizadas por el uno o más procesadores controlan adicionalmente la arquitectura configurada del sistema informático para realizar lo siguiente en respuesta a recibir una solicitud para realizar una operación en la localización del sistema de ficheros particular:

identificar un estado de localización asociado con un solicitante de la solicitud;
identificar datos de caducidad que corresponden al estado de localización, y que está asociado con la operación solicitada; y
usar los datos de caducidad identificados para determinar si la operación solicitada está permitida en la entidad de sistema de ficheros;
en el que, si se determina que la operación solicitada no está permitida, las instrucciones ejecutables por ordenador controlan adicionalmente la arquitectura configurada del sistema informático para realizar lo siguiente:

determinar si la entidad de sistema de ficheros se ha de borrar automáticamente basándose en una entrada de un campo de indicador de borrado asociado con los datos de caducidad de operación; y en caso afirmativo, borrar automáticamente la entidad de sistema de ficheros.

10. El sistema informático de acuerdo con la reivindicación 9, en el que la entidad de sistema de ficheros particular es un fichero.

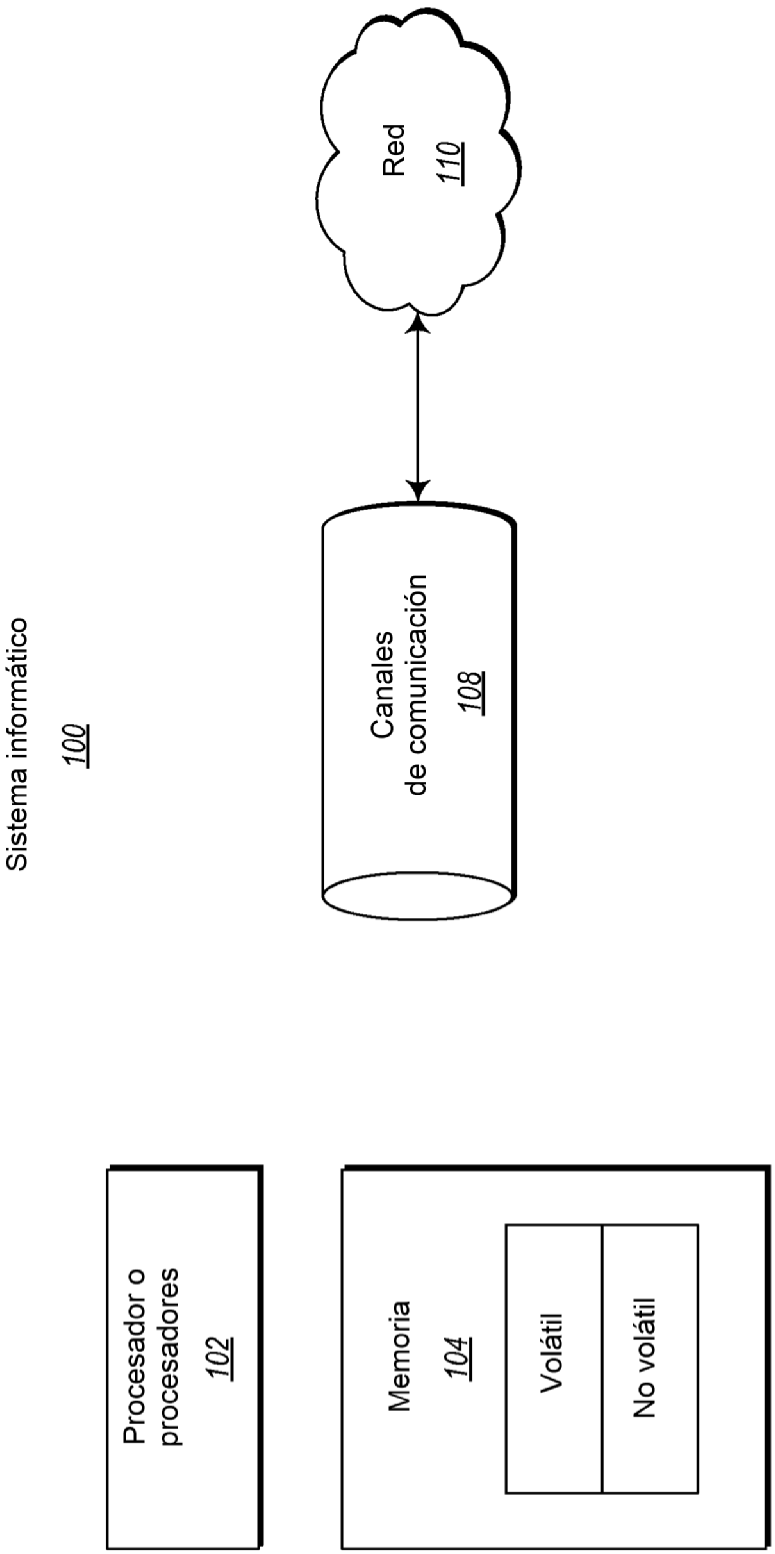
Sistema informático
100
Red
110
Canales
de comunicación
108
Procesador o
procesadores
102
Memoria
104
Volátil
No volátil

Figura 1

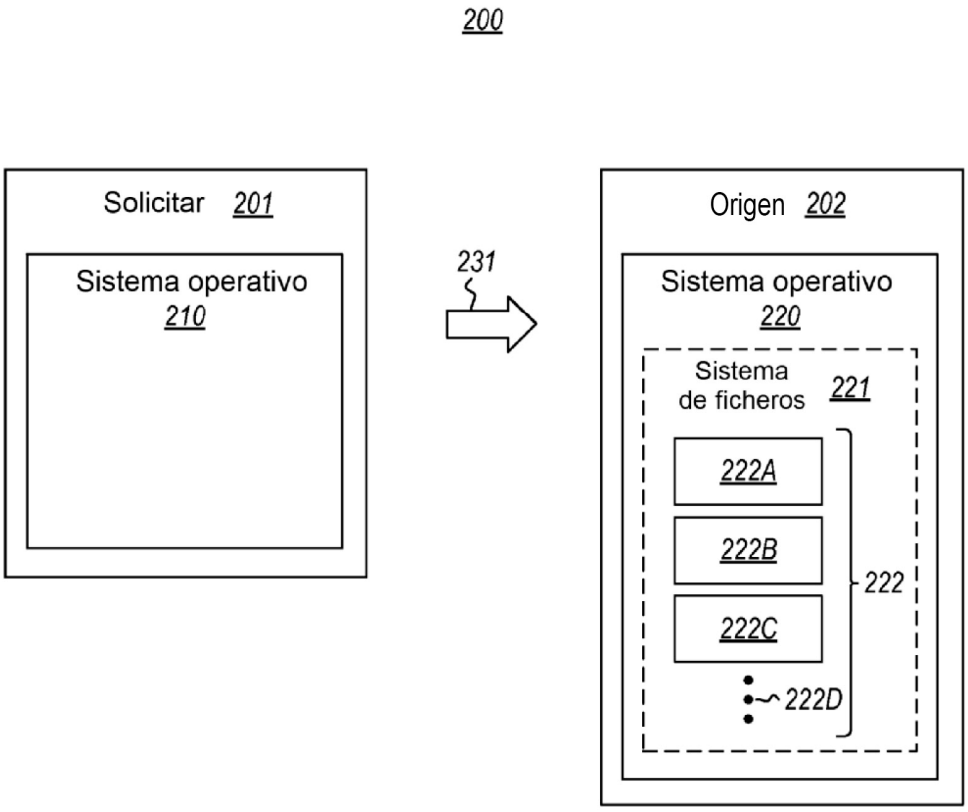

Figura 2

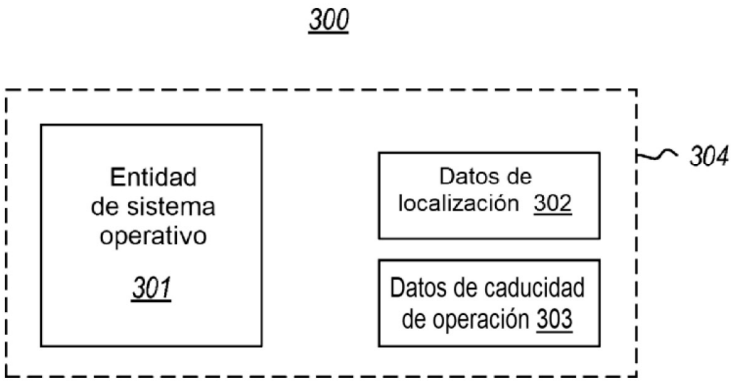

Figura 3

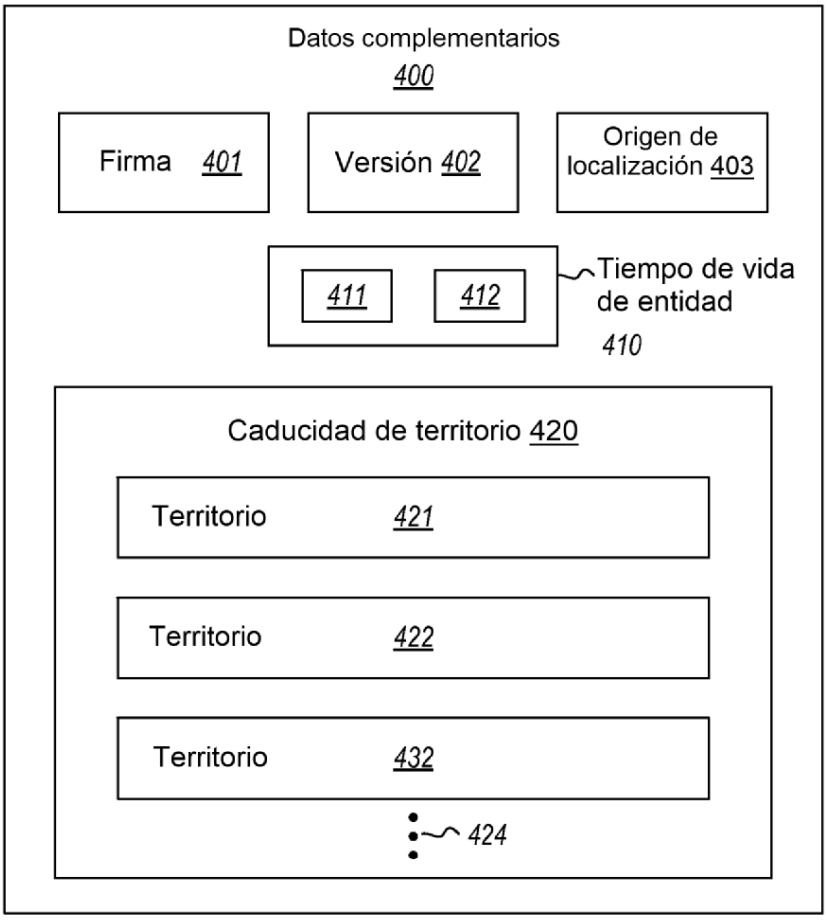

Figura 4

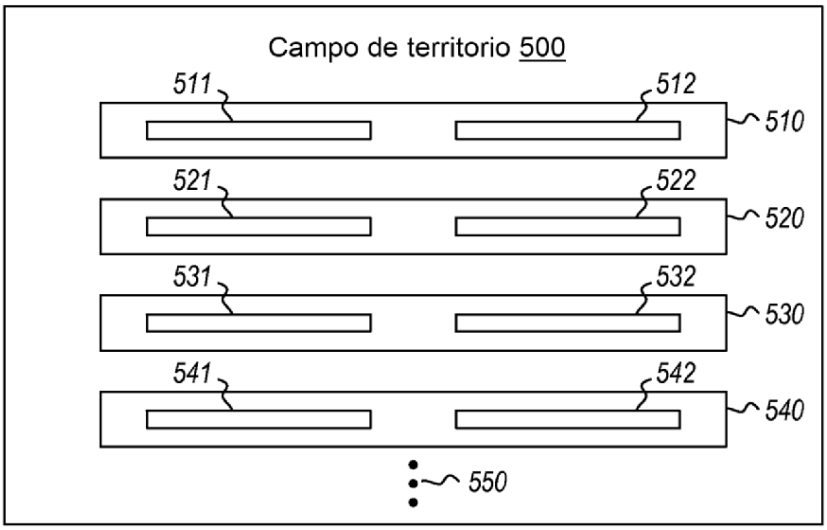

Figura 5

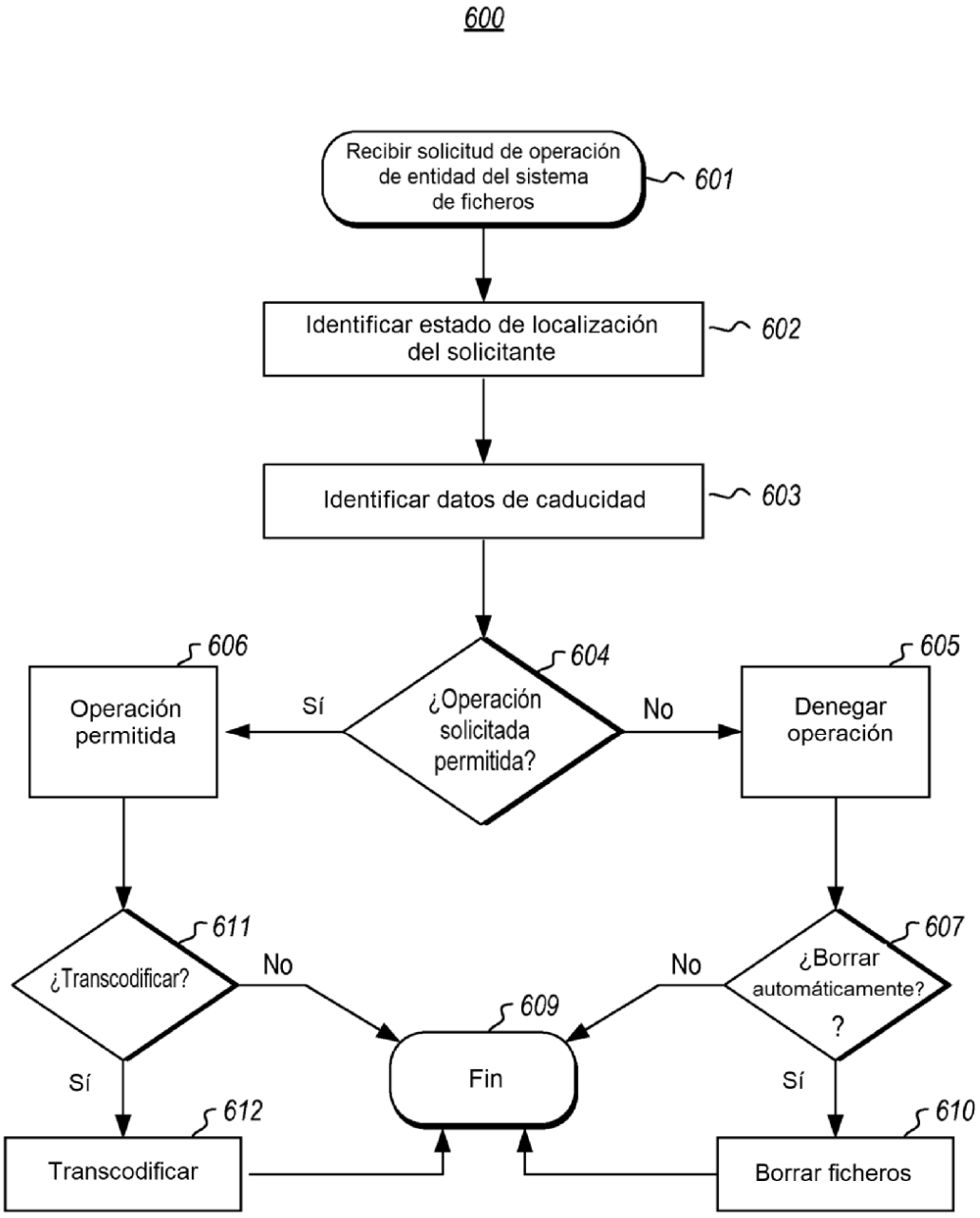
600
Recibir solicitud de operación de entidad del sistema de ficheros
601
Identificar estado de localización del solicitante
602
Identificar datos de caducidad
603
¿Operación solicitada permitida?
604
Sí
No
Operación permitida
606
Denegar operación
605
¿Transcodificar?
611
No
Sí
¿Borrar automáticamente?
607
No
Sí
Fin
609
Transcodificar
612
Borrar ficheros
610

Figura 6

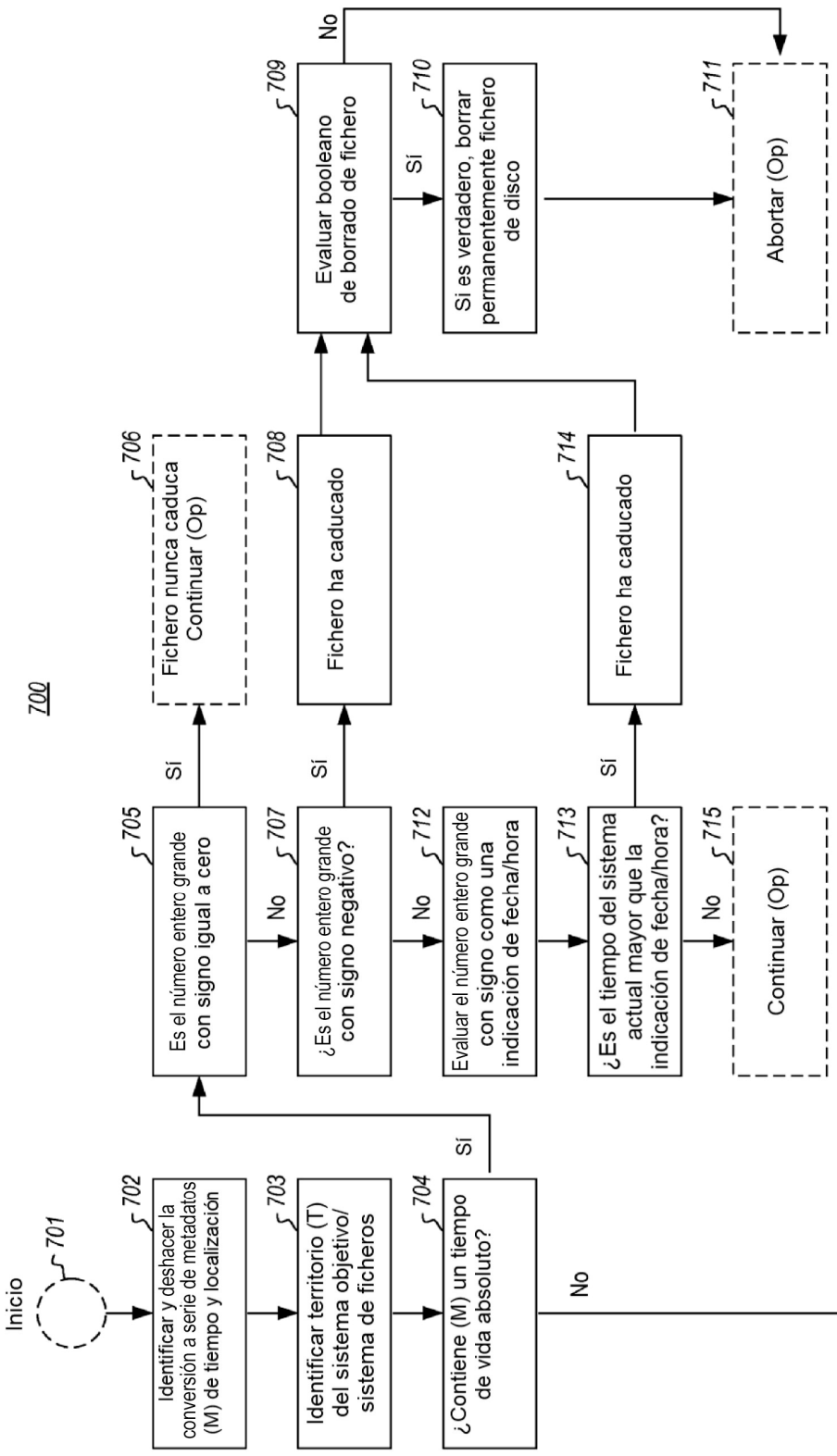
700
Inicio
701
Identificar y deshacer la conversión a serie de metadatos (M) de tiempo y localización
702
Identificar territorio (T) del sistema objetivo/ sistema de ficheros
703
¿Contiene (M) un tiempo de vida absoluto?
704
Si
No
Continuar a n.º 716
Es el número entero grande con signo igual a cero
705
Si
Fichero nunca caduca Continuar (Op)
706
No
¿Es el número entero grande con signo negativo?
707
Si
Fichero ha caducado
708
No
Evaluar el número entero grande con signo como una indicación de fecha/hora
712
Si
Fichero ha caducado
714
No
¿Es el tiempo del sistema actual mayor que la indicación de fecha/hora?
713
No
Continuar (Op)
715
Evaluar booleano de borrado de fichero
709
Si
Si es verdadero, borrar permanentemente fichero de disco
710
No
Abortar (Op)
711

Figura 7

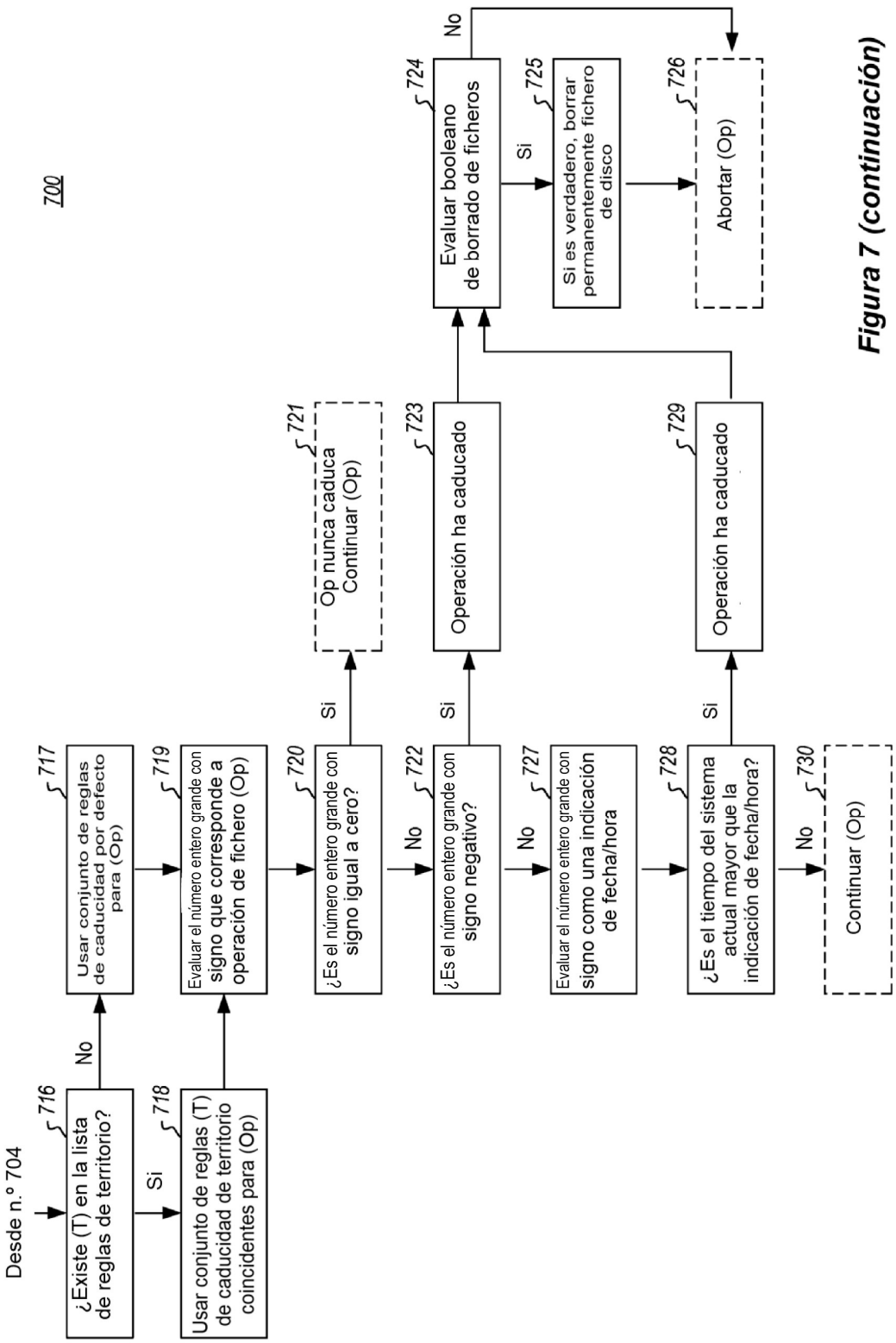

Figura 7 (continuación)